

UNCLASSIFIED

AD 406 911

DEFENSE DOCUMENTATION CENTER

FOR

SCIENTIFIC AND TECHNICAL INFORMATION

CAMERON STATION, ALEXANDRIA, VIRGINIA



UNCLASSIFIED

NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

CATALOGED BY DDC  
AS AD No. 406911

406 911

63-4-1

ON HOMOMORPHIC IMAGES OF TRANSITION GRAPHS

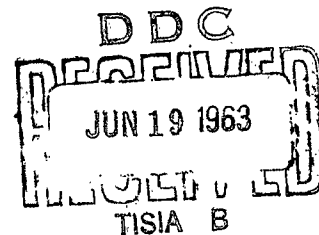
by

Michael Yoeli and Abraham Ginzburg  
Technion, Israel Institute of Technology, Haifa, Israel

Technical Report No. 11

This report was prepared for the  
U. S. OFFICE OF NAVAL RESEARCH, INFORMATION SYSTEMS BRANCH  
under Contract No. N62558-3510

Jerusalem, Israel  
April, 1963



# ON HOMOMORPHIC IMAGES OF TRANSITION GRAPHS

by

Michael Moeli and Abraham Ginzburg  
Technion, Israel Institute of Technology, Haifa, Israel

Technical Report No. 11

This report was prepared for the  
U. S. OFFICE OF NAVAL RESEARCH, INFORMATION SYSTEMS BRANCH  
under Contract No. N62558-3510

Jerusalem, Israel

April, 1963

## I. INTRODUCTION

The concept of transition graph has been introduced in [1] in connection with sequential machine decompositions. It has been shown there that the study of homomorphic images of transition graphs does facilitate the derivation of all admissible partitions (also called partitions having the substitution property [2, 3]) of a sequential machine.

In this report a simple method is derived for obtaining all homomorphic images of a given complete or partial transition graph.

This method consists of the successive application of elementary steps, corresponding to four types of "elementary" congruences.

Furthermore, it is shown that the number of elementary steps required to derive a given homomorphic image is constant, if the original transition graph is complete and connected.

## II. BASIC CONCEPTS

A (transition) graph  $G$  is a couple  $(S, \Gamma)$ , where  $S$  is a finite set of vertices and  $\Gamma$  a map of a non-empty subset  $S_1$  of  $S$  into  $S$ .

If  $S_1 = S$ , the graph is complete, otherwise partial.

The graph  $G' = (S', \Gamma')$  is a homomorphic image of the graph  $G = (S, \Gamma)$  if there exists a map  $\varphi$  of  $S$  onto  $S'$  such that:

$$\Gamma' = \psi^{-1} \Gamma \psi \quad *)$$

We shall use the notation  $G' = G\psi$ .

A cycle  $C$  of length  $k$  of  $G$  is a sequence  $C = (s_0, s_1, \dots, s_{k-1})$  of  $k$  different vertices of  $G$ , such that

$$s_{i-1} \Gamma = s_i, \quad (i = 1, 2, \dots, k-1) \text{ and } s_{k-1} \Gamma = s_0.$$

The vertex  $s$  of a partial  $G$  is a sink, if  $s \in S - S_1$ .

Every graph consists of one or more separate connected parts. Each such part contains either a single cycle or a single sink.

The equivalence relation  $E$  on  $S$  is a congruence on  $G(S, \Gamma)$  if

$$s, t \in S_1 \text{ and } s \equiv t(E) \Rightarrow s\Gamma \equiv t\Gamma(E), \text{ i.e., if } \Gamma^{-1}E\Gamma \subseteq E.$$

Such a congruence determines the factor graph  $G/E = (\bar{S}, \bar{\Gamma})$ , where  $\bar{S} = S/E$  and  $\bar{\Gamma} = \psi^{-1} \Gamma \psi$ ,  $\psi$  denoting the natural mapping of  $S$  onto  $\bar{S}$ .

Evidently,  $G/E$  is a homomorphic image of  $G$ .

Conversely, if  $G' = G\psi$  and  $E$  is the equivalence relation on  $S$  determined by  $\psi$ , then  $E$  is a congruence on  $G$  and  $G/E$  is isomorphic to  $G'$ .

---

\*)  $\psi^{-1} \Gamma \psi$  denotes the relational product of the relations  $\psi^{-1}$ ,  $\Gamma$ , and  $\psi$ .

Let  $E_1$  and  $E_2$  be equivalences on the set  $S$  such that  $E_1 \supset E_2$ . We define the equivalence relation  $E = E_1/E_2$  on  $S/E_2$  in the natural way: two  $E_2$ -classes belong to the same  $E$ -class, if and only if they are both subsets of the same  $E_1$ -class.

Obviously, if  $E = E_1/E_2$ ,  $E_1$  is uniquely determined by  $E$  and  $E_2$  (notation:  $E_1 = E_2 * E$ ).

The following lemma is proved in [4]:

Lemma 1. Let  $E_1, E_2$  be congruences on  $G$  such that  $E_1 \supset E_2$ . Then  $E_1/E_2$  is a congruence on  $G/E_2$  and  $G/E_2/E_1/E_2 \cong G/E_1$ .

It is also easily verified that if  $E_2$  is a congruence on  $G$ , and  $E$  on  $G/E_2$ , then  $E_1 = E_2 * E$  is a congruence on  $G$ . If  $E$  is non-trivial,  $E_1$  properly includes  $E_2$ .

### III. ELEMENTARY CONGRUENCES

The following four types of equivalence relations on  $S$ , the set of vertices of a given graph  $G$ , are easily verified to be congruences on  $G$ . They will be called elementary congruences (on  $G$ ).

Type  $E_{\alpha}$ . Let  $(s^{\cap 0} = s, s^{\cap 1}, \dots, s^{\cap k-1})$  be a cycle of length  $k$  and  $p$  a prime divisor of  $k$ .

Then  $s^{\cap i} \equiv s^{\cap j} (E_{\alpha}) \iff i \equiv j \pmod{\frac{k}{p}}$ .

Type  $E_3$ . Let  $s$  and  $t$  be vertices such that  $s \equiv t$ .

Then  $s \equiv t (E_3)$ .

Type  $E_4$ . Let  $C_1$  and  $C_2$  be different cycles, both of length  $k$ , and let  $s_1, s_2$  be arbitrary vertices of  $C_1, C_2$ , respectively.

Then  $s_1 \equiv s_2 (E_4)$  ( $j = 0, 1, \dots, k-1$ ).

Type  $E_5$ . Let  $s$  be a sink, and  $t$  an arbitrary vertex.

Then  $s \equiv t (E_5)$ .

We shall denote the identity congruence as  $\Delta$ . Also we shall write  $E_1 \supset E_2$  to indicate that  $E_1$  includes  $E_2$  properly.

Theorem 1. A congruence  $E \neq \Delta$  on a given graph  $G$  is elementary if and only if for every congruence  $E'$  on  $G$

$$E \supset E' \Rightarrow E' = \Delta.$$

Proof. Evidently, if  $E$  is an elementary congruence, it does not properly include any congruence  $E' \neq \Delta$  on  $G$ .

Conversely, assume  $E \neq \Delta$  and  $E \not\supset E'$ , for every congruence  $E' \neq \Delta$  on  $G$ .

There exist two vertices  $s, t$  such that  $s \equiv t (E)$ . We shall distinguish between five cases (A-E) where A, B, C cover the alternative that  $s$  and

$t$  belong to the same connected part of  $G$ ;  $D, E, \dots$   $s$  and  $t$  belong to different parts of  $G$ .

Case A. There exists a positive integer  $h$  such that  $s \Gamma^h = t \Gamma^h$ .

Then the congruence  $E'$  defined by:

$$s \Gamma^{h-1} \equiv t \Gamma^{h-1} (E')$$

is elementary of type  $E_\beta$  and  $E \approx E' \neq \Delta$ . Hence  $E = E'$ .

Case B. There exists a non-negative integer  $h$  such that

$s \Gamma^h = u \neq v = t \Gamma^h$  and  $u, v$  are both on the same cycle  $C$  (of length  $k$ ).

Let  $v = u \Gamma^m$ , let  $d$  be the greatest common divisor (g. c. d.) of  $m$  and  $k$ , and  $p$  a prime number dividing  $\frac{k}{d}$ . We define the elementary congruence  $E'$  of type  $E_\alpha$  by

$$u \Gamma^i \equiv u \Gamma^j (E') \iff i \equiv j \pmod{\frac{k}{p}}.$$

Then  $E \approx E' \neq \Delta$ . Thus  $E = E'$ , i. e.,  $E$  is elementary.

Case C. The vertices  $s$  and  $t$  belong to the same connected part of the graph, without satisfying the conditions of cases A and B. Thus, there exist non-negative integers  $h_1 \neq h_2$  such that  $s \Gamma^{h_1} = t \Gamma^{h_2}$  is a sink.

Say  $h_1 > h_2$ . Then the congruence  $E'$  defined by  $s \Gamma^{h_1} \equiv t \Gamma^{h_2} (E')$  is elementary, of type  $E_0$ , and satisfies  $E \approx E' \neq \Delta$ . Hence  $E = E'$ .

Case D. The vertices  $s$  and  $t$  belong to two different connected

parts, containing cycles  $C_1$  and  $C_2$  of length  $k_1$  and  $k_2$  respectively.

Then there exists a non-negative integer  $h$  such that  $s \cap^h = u \equiv v = t \cap^h(E)$  and  $u \in C_1$ ,  $v \in C_2$ . Let  $d$  be the g.c.d. of  $k_1$  and  $k_2$ . If, say,  $k_1 > d$  then the congruence  $E'$  given by

$$u \cap^i \equiv u \cap^j(E') \iff i \equiv j \pmod{d}$$

is properly included in  $E$ . Hence  $k_1 = k_2 = d$ , and the elementary congruence  $E''$  of type  $E_\gamma$  merging cycles  $C_1$  and  $C_2$  satisfies  $E \supseteq E'' \neq \Delta$ .

Therefore,  $E = E''$ , i.e.,  $E$  is elementary.

Case E. The vertices  $s$  and  $t$  belong to separate connected parts and there exists an integer  $h \geq 0$ , such that  $s \cap^h$  (or alternatively  $t \cap^h$ ) is a sink, whereas  $t \cap^j$  ( $s \cap^j$  respectively)  $j < h$ , is not a sink.

Then  $E'$ , defined by  $s \cap^h \equiv t \cap^h(E')$  is elementary (type  $E_\gamma$ ), and  $E \supseteq E' \neq \Delta$ . Hence  $E = E'$ .

Theorem 1 is thus proved.

Theorem 2. If  $G'$  is a homomorphic image of  $G$ , there exists a series

$$G = G_0, G_1, \dots, G_r \cong G' \quad (1)$$

such that  $G_{i+1}$  ( $i = 0, 1, 2, \dots, r-1$ ) is a homomorphic image of  $G_i$  and the congruence on  $G_i$  determined by  $G_{i+1}$  is elementary.

Proof. Let  $E$  be the congruence on  $G$  determined by  $G'$ . If  $E$  is elementary, there is nothing to prove. Otherwise, by Theorem 1,

there must exist an elementary congruence  $E_1$ , such that  $E \supset E_1 \supset \Delta$ .

$G_1 = G/E_1$  is a proper homomorphic image of  $G$ , and, by Lemma 1,

$$G/E_1/E/E_1 \cong G/E \cong G'.$$

Hence  $G'$  is a homomorphic image of  $G_1$ . Replacing  $G$  by  $G_1$  in the above reasoning, we obtain a graph  $G_2 = G_1/E_2$  where  $E_2$  is elementary and  $G'$  is a homomorphic image of  $G_2$ .

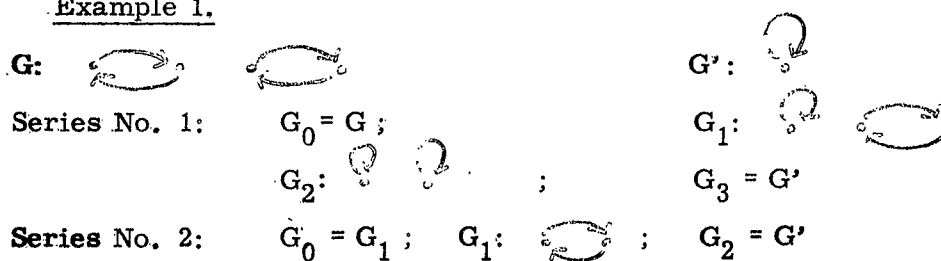
Continuing this process, which must terminate after a finite number of steps, the series (1) is obtained.

#### IV. JORDAN-DEDEKIND CHAIN CONDITIONS

A series of type (1) is clearly refined, i.e., no additional graph  $G_j$  can be inserted between any two elements of the series, such that the new series still satisfies the conditions of Theorem 2.

Generally, given  $G$  and  $G'$ , there exists a number of essentially different refined series from  $G$  to  $G'$ . The following two examples show that such series may even be of different lengths.

##### Example 1.



Example 2.

$G: \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet$

$G': \bullet \rightarrow \bullet$

Series No 1:  $G = G_0$ ,

$G_1: \bullet \rightarrow \bullet \rightarrow \bullet$ ,  $G_2 = G'$

Series No 2:  $G = G_0$ ,

$G_1: \bullet \rightarrow \bullet \rightarrow \bullet$ ,

$G_2: \bullet \rightarrow \bullet \rightarrow \bullet$ ,  $G_3 = G'$

However, for connected, complete graphs the following holds:

Theorem 3. Let  $G$  be a complete, connected graph and  $G'$  a homomorphic image of  $G$ . Then every refined series of type (1) from  $G$  to  $G'$  is of the same length.

Proof. Let  $G = G_0, G_1, \dots, G_r = G'$  be a series of the required type and

$$E_1, E_2, \dots, E_r \quad (2)$$

the corresponding congruences. It follows from the proof of Theorem 1, that each  $E_i$  is either of type  $E_\alpha$  or  $E_\beta$ .

Now, let  $n_i$  be the number of vertices of  $G_i$  and  $k_i$  its cycle length.

If  $E_i$  is of type  $E_\beta$ ,  $k_i = k_{i-1}$ , and  $n_i = n_{i-1} - 1$ .

If  $E_i$  is of type  $E_\alpha$ , then  $\frac{k_{i-1}}{k_i}$  is prime.

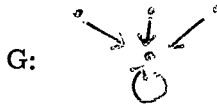
Let now  $\frac{k_0}{k_r} = p_1^{h_1} p_2^{h_2} \dots p_m^{h_m}$  be the decomposition of  $\frac{k_0}{k_r}$  into prime factors. Then the number of  $E_i$  of type  $E_\alpha$  in (2) equals

$$h_\alpha = h_1 + h_2 + \dots + h_m.$$

Now the  $E_{\rho}$  steps have to decrease the number of vertices by  $h_{\rho} = (n_0 - k_0) - (n_r - k_r)$ . Thus  $r = h_{\alpha} + h_{\rho}$ , i.e.,  $r$  is independent of the particular series chosen.

It follows from Theorem 3 that the lattice of congruences of a complete, connected graph satisfies the Jordan-Dedekind chain condition. However, this lattice is in general not modular, as shown by the following

Example 3.



The lattice of congruences of  $G$  coincides with the lattice of equivalences of the set of its vertices, which is known to be non-modular.

V. CONCLUSIONS

Considering applications to sequential machines (finite automata), we have obtained in this report a direct method to derive all admissible partitions of a single-input, complete or partial machine.

Although this method is also useful in connection with multiple-input machines, the derivation of an efficient algorithm to obtain all admissible partitions of such a machine requires further investigations.

REFERENCES

- [1] M. Yoeli, "The Cascade Decompositions of Sequential Machines,"  
IRE Trans. on Electronic Computers, EC -10, 587-592, Dec., 1961.
  
- [2] J. Hartmanis, "Symbolic Analysis of a Decomposition of Information  
Processing Machines," Inf. and Control, 3, 154-178, June, 1960.
  
- [3] J. Hartmanis, "On the State Assignment Problem for Sequential  
Machines, I," IRE Trans. on Electronic Computers, EC-10, 157-165,  
June, 1961.
  
- [4] M. Yoeli, "Decompositions of Finite Automata," Technical Report  
No. 10, Hebrew University, Jerusalem, Israel, March, 1963.